2025/1550

29.7.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/1550,

28. juuli 2025,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruses (EL) 2023/1543 osutatud detsentraliseeritud IT-süsteemi tehniline kirjeldus ja muud nõuded

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 12. juuli 2023. aasta määrust (EL) 2023/1543, mis käsitleb Euroopa andmeesitamismäärust ja Euroopa andmesäilitamismäärust elektrooniliste tõendite hankimiseks kriminaalmenetluses ja kriminaalmenetluse järgsete vabadusekaotuslike karistuste täitmisele pööramiseks, ([1]) eelkõige selle artikli 25 lõike 1 punkte a, b, c ja d,

ning arvestades järgmist:

(1) Määruses (EL) 2023/1543 osutatud detsentraliseeritud IT-süsteemi loomiseks on vaja kindlaks määrata ja vastu võtta tehniline kirjeldus, meetmed ja eesmärgid kõnealuse süsteemi rakendamiseks.

(2) Vastavalt määrusele (EL) 2023/1543 peaks detsentraliseeritud IT-süsteem koosnema liikmesriikide ning liidu asutuste ja organite IT-süsteemidest ja neid omavahel siduvatest koostalitlevatest e-CODEXi pääsupunktidest. Detsentraliseeritud IT-süsteemi tehniline kirjeldus ja muud nõuded peaksid seega kajastama seda raamistikku.

(3) Vastavalt määrusele (EL) 2023/1543 peaksid detsentraliseeritud IT-süsteemi pääsupunktid põhinema Euroopa Parlamendi ja nõukogu määruse (EL) 2022/850 ([2]) artikli 3 punktis 3 määratletud volitatud e-CODEXi pääsupunktidel.

(4) Liikmesriigid võivad otsustada riikliku süsteemi asemel kasutada oma tagasüsteemina komisjoni arendatud etalonteostuse tarkvara. Koostalitlusvõime tagamiseks peaksid nii riiklikud IT-süsteemid kui ka etalonteostuse tarkvara vastama samadele käesolevas määruses sätestatud tehnilistele kirjeldustele ja nõuetele.

(5) Detsentraliseeritud IT-süsteemi jõudluse ja töökindlusega seotud võimalike tehniliste probleemide leevendamiseks on vaja kehtestada selle süsteemi kaudu edastatavate elektrooniliste tõendite mahu piirmäär. Pärast süsteemi kasutuselevõtmist tuleks jälgida tõendite edastamise sagedust ja mahtu ning süsteemi tõhususe maksimeerimiseks tuleks seda piirmäära vajaduse korral kohandada.

(6) Detsentraliseeritud IT-süsteemi koostalitlusvõime ja tõhususe tugevdamiseks tuleks teha kohustuslikuks asjakohaste ETSI standardite kasutamine. Jälgida tuleks olukorra edasist arengut ja vajaduse korral tuleks kaaluda täiendavate ETSI standardite vastuvõtmist.

(7) Määrus (EL) 2023/1543 on Iirimaale siduv ja seepärast osaleb ta käesoleva määruse vastuvõtmisel.

(8) Euroopa Liidu lepingule ja Euroopa Liidu toimimise lepingule lisatud Taani seisukohta käsitleva protokolli nr 22 artiklite 1 ja 2 kohaselt ei ole käesolev määrus Taani suhtes siduv ja seda ei kohaldata Taanis.

([1]) ELT L 191, 28.7.2023, lk 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

([2]) Euroopa Parlamendi ja nõukogu 30. mai 2022. aasta määrus (EL) 2022/850, milles käsitletakse arvutipõhist süsteemi piiriüleseks elektrooniliseks andmevahetuseks tsiviil- ja kriminaalasjades tehtava õigusalase koostöö valdkonnas (e-CODEXi süsteem) ning millega muudetakse määrust (EL) 2018/1726 (ELT L 150, 1.6.2022, lk 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([3]) artikli 42 lõikele 1 konsulteeriti Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 25. juunil 2025.

(10) Käesoleva määrusega ettenähtud meetmed on kooskõlas määruse (EL) 2023/1543 artikli 26 kohaselt asutatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Detsentraliseeritud IT-süsteemi tehniline kirjeldus

Detsentraliseeritud IT-süsteemi tehniline kirjeldus ning nõuded, meetmed ja eesmärgid, millele on osutatud määruse (EL) 2023/1543 artikli 25 lõikes 1 ja mis on vajalikud teabevahetuseks kõnealuse määruse artikli 19 tähenduses, on sätestatud käesoleva määruse lisas.

Artikkel 2

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja liikmesriikides vahetult kohaldatav kooskõlas aluslepingutega.

Brüssel, 28. juuli 2025

Komisjoni nimel
president
Ursula VON DER LEYEN

([3]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

LISA

DETSENTRALISEERITUD IT-SÜSTEEMI TEHNILINE KIRJELDUS

(osutatud artiklis 1)

1. **Sissejuhatus ja rakendusala**

Käesolevas lisas on sätestatud määruses (EL) 2023/1543 osutatud menetlusteks kasutatava detsentraliseeritud IT-süsteemi tehniline kirjeldus, meetmed ja eesmärgid.

Määruse (EL) 2023/1543 ja täpsemalt selle artikli 19 kohaselt peab detsentraliseeritud IT-süsteem võimaldama kirjalikku teabevahetust pädevate asutuste ja määratud majandusüksuste või esindajate vahel, pädevate asutuste vahel ning pädevate asutuste ja liidu pädevate asutuste või organite vahel.

2. **Mõisted**

2.1. „HTTPS“ (Hypertext Transfer Protocol Secure) ehk „turvaline hüperteksti edastuse protokoll“ – krüpteeritud side ja turvalised sidekanalid;

2.2. „päritolu salgamise vääramine“ – meetmed, mille abil tõendatakse andmete terviklust ja päritolu, kasutades selliseid meetodeid nagu digitaalne sertifitseerimine, avaliku võtme taristu ning e-allkirjad ja e-templid;

2.3. „kättesaamise salgamise vääramine“ – meetmed, mille abil andmete lähetajale tõendatakse andmete kättesaamist andmete kavandatud saaja poolt, kasutades selliseid meetodeid nagu digitaalne sertifitseerimine, avaliku võtme taristu ning e-allkirjad ja e-templid;

2.4. „SOAP“ (Simple Object Access Protocol) ehk lihtne objektipöörduse protokoll – arvutivõrkudes veebiteenuste rakendamisel struktureeritud teabe vahetamiseks kasutatav Veebikonsortsiumi standardite kohane sõnumivahetus-protokoll;

2.5. „REST“ (Representational State Transfer) ehk esitusoleku siire – veebirakenduste kavandamise arhitektuuristiil, mis põhineb olekukontrollita kliendi-serveri sidemudelil ja mille puhul kasutatakse standardmeetodeid ressurssidega toimingute tegemiseks, mis on tavaliselt struktureeritud vormingus;

2.6. „veebiteenus“ – tarkvarasüsteem, mis on loodud masinatevahelise koostalitlusvõimelise võrgupõhise suhtluse toetamiseks ja millel on masintöödeldavas vormingus kirjeldatud liides;

2.7. „andmevahetus“ – sõnumite, vormide, dokumentide ja elektrooniliste tõendite vahetamine detsentraliseeritud IT-süsteemi kaudu;

2.8. „rakendusliides“ – ühisel andmevahetusstandardil põhinev rakendusliides, mis võimaldab teenuseosutajatel, kes kasutavad kohandatud IT-lahendusi elektrooniliste tõendite taotlustega seotud teabe ja andmete vahetamiseks, saada detsentraliseeritud IT-süsteemidele automaatse juurdepääsu;

2.9. „veebipõhine liides“ – HTTPSi kaudu internetis kättesaadav kasutajaliides, mis võimaldab teenuseosutajatele detsentraliseeritud IT-süsteemile käsitsi juurdepääsu, et ametiasutustega turvaliselt elektrooniliste tõendite taotlustega seotud teabe ja andmete vahetamise eesmärgil suhelda, ilma et nad peaksid looma oma spetsiaalse taristu;

2.10. „ETSI standardid“ – Euroopa Telekommunikatsioonistandardite Instituudi (ETSI) väljatöötatud tehnilised kirjeldused ja standardid, mille eesmärk on tagada info- ja kommunikatsioonitehnoloogia koostalitlusvõime, turvalisus ja tõhusus. Need hõlmavad raamistikke, protokolle ja parimaid tavasid mitmesuguste tehnoloogiliste lahenduste, sealhulgas mobiilsidevõrkude, raadioside, küberturvalisuse ja internetitaristu jaoks;

2.11. „räsi“ – kindla pikkusega väljund, mis luuakse krüptograafilise räsifunktsiooni rakendamisel suvalise pikkusega sisendi suhtes. Krüptograafiline räsifunktsioon on kavandatud tagama põhilisi turvaomadusi, sealhulgas originaalikindlust, lisaoriginaalikindlust ja kollisioonikindlust, vältides räsi ümberpööramist ja kaitstes kollisioonrünnete eest;

2.12. „e-CODEXi süsteem“ – määruse (EL) 2022/850 artikli 3 punktis 1 määratletud e-CODEXi süsteem;

2.13. „ELi e-õiguskeskkonna põhisõnastik“ – määruse (EL) 2022/850 lisa punktis 4 määratletud ELi e-õiguskeskkonna põhisõnastik;

2.14. „ebMS“ (ebXML Message Service) – OASISe raames välja töötatud sõnumivahetusprotokoll, mis võimaldab e-äri dokumentide turvalist, usaldusväärset ja koostalitlusvõimelist vahetamist SOAPi abil, toetades ettevõtjatevahelist integreerimist eri süsteemide vahel;

2.15. „AS4“ (Applicability Statement 4) – OASISe standard, mis kirjeldab ebMS 3.0 ning lihtsustab turvalist ja koostalitlusvõimelist ettevõtjatevahelist sõnumivahetust, kasutades avatud standardeid, nagu SOAP ja WS-Security;

2.16. „taaste sihtkestus“ – maksimaalne lubatav aeg intsidendi järel teenuse taastumiseks ilma andmekaota;

2.17. „taaste sihtseis“ – maksimaalne aktsepteeritav andmekadu tõrke korral.

3. **Elektroonilise teabevahetuse meetodid**

3.1. Kirjalikuks teabevahetuseks liikmesriikide pädevate asutuste vahel, pädevate asutuste ja teenuseosutajate määratud majandusüksuste või esindajate vahel ning pädevate asutuste ja liidu asutuste või organite vahel kasutatakse detsentraliseeritud IT-süsteemis andmevahetuse eesmärgil teenusepõhiseid sidemeetodeid, näiteks veebiteenuseid või muid taaskasutatavaid komponente ja tarkvaralahendusi. Täpsemalt hõlmab see teabevahetust e-CODEXi süsteemi pääsupunktide kaudu, nagu on sätestatud määruse (EL) 2022/850 artikli 5 lõikes 2. Seega peab detsentraliseeritud IT-süsteem toimiva ja koostalitlusvõimelise piiriülese andmevahetuse tagamiseks toetama teabevahetust e-CODEXi süsteemi kaudu.

3.2. Võttes arvesse vastavalt määruse (EL) 2023/1543 artikli 19 lõigetele 1 ja 4 Euroopa andmeesitamismääruste alusel detsentraliseeritud IT-süsteemi kaudu edastatavate elektrooniliste tõendite eeldatavat suurt mahtu, mis võib põhjustada tehnilise jõudluse piiranguid, mis võivad detsentraliseeritud IT-süsteemi negatiivselt mõjutada, edastatakse elektroonilisi tõendeid selle süsteemi kaudu juhul, kui nende maht ei ületa 25 megabaiti (25 600 kilobaiti). Seda piirmäära ületavaid elektroonilisi tõendeid edastatakse vastavalt kõnealuse määruse artikli 19 lõikele 5.

3.3. Kui vastavalt määruse (EL) 2023/1543 artikli 19 lõikele 6 edastatakse teavet alternatiivsete vahenditega, kuna detsentraliseeritud IT-süsteemi ei saa kasutada mõnel kõnealuse määruse artikli 19 lõikes 5 nimetatud põhjusel, toimitakse järgmiselt.

3.3.1. Kui teabe edastamine puudutab pädevate asutuste ja teenuseosutajate vahelist kirjalikku teabevahetust, sealhulgas vormide vahetamist määruse (EL) 2023/1543 artikli 19 lõike 1 tähenduses, registreerib edastaja edastamise oma riiklikus IT-süsteemis, mis on detsentraliseeritud IT-süsteemi osa. Registreeritud teave sisaldab vähemalt juhtumi või toimiku viitenumbrit, kuupäeva ja kellaaega, saatjat ja saajat ning faili nime ja suurust.

3.3.2. Kui teabe edastamine puudutab pädevate asutuste vahelist kirjalikku teabevahetust, sealhulgas vormide vahetamist, või kirjalikku teabevahetust pädevate liidu asutuste või organitega määruse (EL) 2023/1543 artikli 19 lõike 4 tähenduses, registreerib edastaja edastamise detsentraliseeritud IT-süsteemis, täpsemalt oma riiklikus IT-süsteemis või asjakohasel juhul liidu pädeva asutuse või organi hallatavas IT-süsteemis. Registreeritud teave sisaldab vähemalt juhtumi või toimiku viitenumbrit, edastamise kuupäeva ja kellaaega, saatjat ja saajat ning faili nime ja suurust.

3.3.3. Kui Euroopa andmeesitamismääruse alusel on elektroonilised tõendid teenuseosutajate ja taotleva riigi pädevate asutuste ([1]) vahel edastatud alternatiivsete sidevahenditega või kui elektroonilised tõendid edastatakse täitvalt asutuselt või ametiisikult taotleva riigi pädevatele asutustele täitmisele pööramise menetluses määruse (EL) 2023/1543 artikli 16 lõike 9 kohaselt alternatiivsete vahendite abil, teeb edastaja järgmist:

a) registreerib ja edastab asutusele, kellele elektroonilised tõendid edastati või kättesaadavaks tehti, manifesti osana järgmise teabe:

1) teave saatja ja saaja kohta;

2) metaandmed, mis seovad esitatud elektroonilised tõendid konkreetse Euroopa andmeesitamismääruse või Euroopa andmesäilitamismäärusega;

3) edastamise kuupäev ja kellaaeg või teave selle kohta, millal elektroonilised tõendid saajale kättesaadavaks tehti;

4) teave edastamisviisi kohta (nt turvaline link, mille kaudu elektroonilised tõendid kättesaadavaks tehti, postiasutuse tõend kättesaamise või kättetoimetamise kohta jne) ([2]);

5) taotlevas riigis kavandatavale saajale edastatud või muul viisil kättesaadavaks tehtud elektrooniliste tõendite täielik(ud) failinimi (-nimed);

6) taotlevas riigis kavandatavale saajale edastatud või muul viisil kättesaadavaks tehtud elektrooniliste tõendite andmemaht;

7) vähemalt üks räsi edastatud või kättesaadavaks tehtud andmetest ning teave kasutatud räsialgoritmi(de) kohta. Räsi moodustamiseks kasutatud räsialgoritm peab olema krüptograafiliselt tugev ja tavapäraselt kasutatav ning sellel ei või olla avalikult teadaolevaid nõrkusi, nagu kollisioonid (nt SHA-512, SHA3–512, BLAKE2 või RIPEMD-160, kuid võib olla ka tugevam, kui tehnoloogia areng seda võimaldab);

b) asjakohasel juhul märgib punktis a osutatud manifestis kuupäeva ja kellaaja, milleni elektroonilised tõendid jäävad kättesaadavaks. Seejuures tuleb jätta taotleva riigi pädevale asutusele elektrooniliste tõendite kättesaamiseks mõistlikult aega ning vastav ajavahemik ei või olla lühem kui 10 kalendripäeva ega pikem kui 45 kalendripäeva alates elektrooniliste tõendite kättesaadavaks tegemisest. Taotleva riigi pädeva asutuse taotlusel võib edastaja märgitud ajavahemikku üksikjuhul pikendada;

c) võib punktis a osutatud manifestis registreerida ja edastada juhtumiga seotud lisateavet või märkusi asutusele, kellele elektroonilised tõendid edastati või kättesaadavaks tehti.

3.4. Määruse (EL) 2023/1543 artikli 28 täitmiseks peab etalonteostuse tarkvara olema programmeeritud nii, et see koguks kõnealuse artikli lõikes 2 osutatud statistikat ja edastaks seda või teeks selle muul viisil kättesaadavaks nii struktureeritud (nt XML) kui ka struktureerimata (nt PDF) andmevormingus. Vastavalt määruse (EL) 2023/1543 artikli 28 lõikele 3 võib liikmesriikide hallatavatest riiklikest portaalidest ([3]) vastavate tehniliste võimaluste olemasolu korral edastada või esitada seda statistikat komisjonile ka automatiseeritult. Komisjon annab välja suunised andmestruktuuri ning statistika kogumise ja edastamise meetodi kohta.

([1]) Suurema selguse huvides märgitakse, et viiteid liikmesriikide pädevatele asutustele tuleb käsitada *mutatis mutandis* ka viidetena liikmesriike esindavatele Eurojusti liikmetele, Euroopa prokuröridele ja Euroopa delegaatprokuröridele, kui neil on liidu ja riigisisese õiguse kohaselt õigus täita samu ülesandeid.

([2]) Tuleks meelde tuletada, et vastavalt artikli 19 lõikele 5 peab alternatiivsete sidevahenditega edastamine vastama nõudele, et teabe edastamine on kiire, turvaline ja usaldusväärne ning võimaldab saajal teha kindlaks teabe ehtsuse.

([3]) Riiklike portaalide all mõeldakse riiklikke IT-süsteeme, mis moodustavad osa määruse (EL) 2023/1543 artikli 3 punktis 21 määratletud detsentraliseeritud IT-süsteemist.

4. **Sideprotokollid**

4.1. Detsentraliseeritud IT-süsteemis kasutatakse turvalisi internetiprotokolle:

a) pädevate asutuste vaheliseks sideks detsentraliseeritud IT-süsteemis,

b) pädevate asutuste ning liidu ametite ja organite vaheliseks sideks detsentraliseeritud IT-süsteemis,

c) pädevate asutuste ja teenuseosutajate vaheliseks sideks rakendusliidese ja veebipõhise liidese kaudu ning

d) sideks kohtute andmebaasiga.

4.2. Struktureeritud andmete ja metaandmete määratlemiseks ja edastamiseks kasutatavad detsentraliseeritud IT-süsteemi komponendid põhinevad terviklikel ja üldtunnustatud valdkondlikel standarditel ja protokollidel, nagu SOAP ja REST, eelkõige nendel, millele viitavad Euroopa standardiorganisatsioonid, näiteks ETSI.

4.3. Transpordi- ja sõnumivahetusprotokollide osas on detsentraliseeritud IT-süsteemi aluseks turvalised standardipõhised protokollid, näiteks:

a) piiriüleseks andmevahetuseks AS4 Profile, mis tagab turvalise ja usaldusväärse sõnumivahetuse krüpteerimise ja salgamatuse abil;

b) HTTPS/REST-põhised rakendusliidesed JSON- ja XML-vorminguid toetavaks teabevahetuseks;

c) väga usaldusväärseks teabevahetuseks SOAP, mis hõlmab autentimiseks ja krüpteerimiseks protokolli WS-Security.

4.4. Sujuva ja koostalitlusvõimelise andmevahetuse tagamiseks vastavad detsentraliseeritud IT-süsteemi kasutatavad sideprotokollid asjakohastele koostalitlusvõime standarditele.

4.5. Vajaduse korral kasutatakse elektrooniliste tõendite XML-skeemides asjakohaseid standardeid või sõnastikke, et võimaldada skeemis määratletud elementide ja tüüpide nõuetekohast valideerimist. Sellised standardid või sõnastikud on näiteks:

a) ELi e-õiguskeskkonna põhisõnastik;

b) kvalifitseerimata andmetüübid;

c) Euroopa Liidu keelekoodide loend.

Samuti võivad XML-skeemid vajaduse korral hõlmata asjakohaseid ETSI standardeid, et kasutada neis sisalduvaid määratlusi.

4.6. Komisjon määrab kindlaks spetsifikatsioonid ühise rakendusliidese jaoks, mille täitvad riigid teevad teenuseosutajatele kättesaadavaks detsentraliseeritud IT-süsteemile juurdepääsu vahendina. See rakendusliides põhineb võimalikult suures ja mõistlikus ulatuses ETSI standardil TS 104 144 („Interface definition for the e-Evidence Regulation (EU) 2023/1543 for National Authorities and Service Providers“).

4.7. Turbe- ja autentimisprotokollide osas on detsentraliseeritud IT-süsteemi aluseks standardipõhised protokollid, näiteks:

a) TLS (transpordikihi turve), mis võimaldab võrkudes krüpteeritud ja autenditud teabevahetust, toetades vastastikust autentimist X.509 digisertifikaatide kaudu;

b) OAuth/OpenID Connect (OIDC) turvaliseks autentimiseks ja volitamiseks;

c) avaliku võtme taristu ja digiallkirjad, mis võimaldavad turvalist võtmekehtestust ja sõnumite tervikluse kontrollimist, kasutades usaldusväärsete sertifitseerimisasutuste väljastatud digisertifikaate (X.509).

5. **Infoturbe eesmärgid ja sellega seotud tehnilised meetmed**

5.1. Tehnilised meetmed, millega tagatakse detsentraliseeritud IT-süsteemi kaudu teabe vahetamisel infotehnoloogilise turvalisuse miinimumstandardid, hõlmavad järgmist:

a) meetmed, millega tagatakse teabe konfidentsiaalsus, muu hulgas turvaliste sidekanalite kasutamisega;

b) meetmed, millega tagatakse andmete (sõnumite, vormide, dokumentide ja elektrooniliste tõendite) terviklus nii jõudeoleku kui ka edastamise ajal;

c) meetmed, millega tagatakse detsentraliseeritud IT-süsteemis teabe saatja päritolu salgamise vääramine ja teabe kättesaamise salgamise vääramine;

d) meetmed, millega tagatakse käideldavus, st pidev juurdepääs teenustele ja andmetele, ning hoitakse ära küberrünnetest või tõrgetest tulenevad katkestused;

e) meetmed, millega tagatakse turvasündmuste logimine vastavalt tunnustatud rahvusvahelistele soovitustele infotehnoloogia turvastandardite kohta;

f) meetmed, millega tagatakse kasutajate autentimine ja volitamine, ning meetmed, millega identifitseeritakse detsentraliseeritud IT-süsteemiga ühendatud süsteemid.

5.2. Detsentraliseeritud IT-süsteemi komponentidega tagatakse turvaline side ja andmeedastus, kasutades krüpteerimist, avalikku võtme taristut koos digisertifikaatidega autentimiseks ja turvaliseks võtmekehtestuseks ning turvalisi sõnumivahetusprotokolle nagu AS4 (ebMS), REST-põhised rakendusliidesed ja SOAP sõnumite konfidentsiaalsuse ja tervikluse säilitamiseks.

5.3. Detsentraliseeritud IT-süsteemi komponendid töötatakse välja lõimitud ja vaikimisi andmekaitse põhimõtte kohaselt ning küberturvalisuse kõrge taseme tagamiseks rakendatakse asjakohaseid haldus-, korralduslikke ja tehnilisi meetmeid.

5.4. Komisjon kavandab, arendab ja hooldab etalonteostuse tarkvara kooskõlas määruses (EL) 2018/1725 sätestatud andmekaitsenõuete ja -põhimõtetega. Komisjoni pakutav etalonteostuse tarkvara võimaldab liikmesriikidel täita Euroopa Parlamendi ja nõukogu määrusest (EL) 2016/679 ([4]) ja Euroopa Parlamendi ja nõukogu direktiivist (EL) 2016/680 ([5]) tulenevaid kohustusi (vastavalt kohaldatavusele).

5.5. Liikmesriigid, kes kasutavad etalonteostuse tarkvarast erinevat riiklikku IT-süsteemi, rakendavad vajalikke meetmeid, et tagada selle vastavus määruse (EL) 2016/679 ja direktiivi (EL) 2016/680 nõuetele (vastavalt kohaldatavusele).

5.6. Seoses oma osalemisega detsentraliseeritud IT-süsteemis rakendavad Eurojust ja Euroopa Prokuratuur vajalikke meetmed, et tagada oma IT-süsteemi vastavus määruse (EL) 2018/1725 ja oma asutamisakti nõuetele.

5.7. Liikmesriigid, Eurojust ja Euroopa Prokuratuur loovad oma vastutusalasse kuuluvate ja detsentraliseeritud IT-süsteemi osaks olevate IT-süsteemide jaoks tugevad ohtude avastamise ja intsidentidele reageerimise mehhanismid, et tagada turvaintsidentide õigeaegne tuvastamine ja leevendamine ning neist taastumine vastavalt ettenähtud korrale.

6. **Elektrooniliste tõendite** ([6]) **krüpteerimine**

6.1. Ilma et see piiraks detsentraliseeritud IT-süsteemi turvameetmete kohaldamist, võivad pädevad asutused Euroopa andmeesitamismääruse tegemisel lisaks esitada spetsiaalse X.509 avaliku sertifikaadi elektrooniliste tõendite asümmeetriliseks krüpteerimiseks.

([4]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

([5]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (ELT L 119, 4.5.2016, lk 89).

([6]) Ebaselguse vältimiseks märgitakse, et mõiste „elektroonilised tõendid“ on piiratud määruse (EL) 2023/1543 artikli 3 punktis 8 esitatud määratlusega.

6.2. Punktis 6.1 osutatud sertifikaatide väljaandmise, haldamise, kontrollimise ja kõigi nendega seotud aspektide ning vastava avaliku võtme taristu eest vastutab üksnes taotlev liikmesriik.

6.3. Ilma et see piiraks tehnoloogia edasisele arengule tuginemist, toetavad avalikud sertifikaadid valdkondlikke standardseid krüpteerimisalgoritme, nagu RSA (Rivest-Shamir-Adleman) või ECDH (Elliptic Curve Diffie-Hellman) elliptiliste kõverate krüptosüsteemi (ECC) jaoks.

6.4. Avalikel sertifikaatidel on asjakohane võtmekasutuse laiendus, näiteks RSA-põhiste sertifikaatide puhul „keyEncipherment“ või „dataEncipherment“ ja ECC-põhiste sertifikaatide puhul „keyAgreement“. Sertifikaadid tehakse kättesaadavaks PEM (Privacy-Enhanced Mail) või DER (Distinguished Encoding Rules) vormingus.

6.5. Kui taotlev asutus või ametiisik on esitanud X.509 avaliku sertifikaadi ja teenuseosutaja saadab vastavalt Euroopa andmeesitamismäärusele esitatavad elektroonilised tõendid, krüpteerib ta elektroonilised tõendid enne nende detsentraliseeritud IT-süsteemi kaudu edastamist vastavalt taotleva riigi esitatud X.509 avalikule sertifikaadile.

6.6. Kui taotlev asutus või ametiisik on esitanud X.509 avaliku sertifikaadi, kuid elektrooniliste tõendite edastamine krüpteeritud kujul ei ole tehnilistel või muudel mõjuvatel põhjustel võimalik, võib teenuseosutaja edastada andmed krüpteerimata kujul, ilma et see piiraks määruse (EL) 2023/1543 artikli 19 lõike 5 kohaldamist. Sellisel juhul esitab teenuseosutaja taotlevale asutusele või ametiisikule põhjendustega selgituse.

7. **Käideldavuse miinimumeesmärgid**

7.1. Liikmesriigid, Eurojust ja Euroopa Prokuratuur tagavad oma vastutusalasse kuuluvate detsentraliseeritud IT-süsteemi komponentide alalise ööpäevaringse käideldavuse, kusjuures tehnilise käideldavuse iga-aastane sihtmäär on vähemalt 98 %, välja arvatud korraline hooldus.

7.2. Komisjon tagab kohtute andmebaasi alalise ööpäevaringse käideldavuse, kusjuures tehnilise käideldavuse iga-aastane sihtmäär on vähemalt 99 %, välja arvatud korraline hooldus.

7.3. Võimaluse korral kavandatakse hooldustööd tööpäevadel ajavahemikku 20.00–7.00 Kesk-Euroopa aja järgi.

7.4. Liikmesriigid, Eurojust ja Euroopa Prokuratuur teavitavad komisjoni ja teisi liikmesriike hooldustöödest järgmiselt:

a) 5 tööpäeva ette, kui hooldustööd võivad põhjustada kuni 4-tunnise käideldamatuse;

b) 10 tööpäeva ette, kui hooldustööd võivad põhjustada 4–12-tunnise katkestuse;

c) 30 tööpäeva ette, kui hooldustööd võivad põhjustada kuni enam kui 12-tunnise katkestuse;

7.5. Kui liikmesriigid, Eurojust või Euroopa Prokuratuur on kehtestanud korralise hoolduse perioodid, teavitavad nad komisjoni ja detsentraliseeritud IT-süsteemis osalejaid sellise kavandatud korralise hoolduse päeva(d)est ja kellaaegadest. Olenemata punktis 7.4 sätestatud kohustustest võivad liikmesriigid, Eurojust või Euroopa Prokuratuur otsustada mitte teavitada komisjoni iga kord, kui nende vastutusalas olevad detsentraliseeritud IT-süsteemi komponendid võivad kindlaksmääratud korralise hoolduse perioodil muutuda käideldamatuks.

7.6. Liikmesriikide, Eurojusti või Euroopa Prokuratuuri vastutusalasse kuuluvate detsentraliseeritud IT-süsteemi komponentide ootamatu tehnilise tõrke korral teavitavad nad komisjoni ja detsentraliseeritud IT-süsteemis osalejaid viivitamata nii tõrkest kui ka eeldatavast taaste ajakavast, kui see on teada.

7.7. Liikmesriigi vastutusalasse kuuluvate detsentraliseeritud IT-süsteemi komponentide hoolduse või ootamatu tehnilise tõrke korral, millel on kahjulik mõju rakendusliidese ja/või teenuseosutajate veebipõhise liidese käideldavusele, teeb asjaomane liikmesriik selle teabe viivitamata kättesaadavaks veebisaidil ja/või edastab selle teabe põhjendamatu viivituseta oma territooriumil tegutsevatele teenuseosutajatele.

7.8. Kohtute andmebaasi ootamatu tehnilise tõrke korral teavitab komisjon viivitamata liikmesriike, Eurojusti ja Euroopa Prokuratuuri andmebaasi käideldamatusest ja ka eeldatavast taaste ajakavast, kui see on teada.

7.9. Teenuse katkemise korral tagavad liikmesriigid, Eurojust ja Euroopa Prokuratuur teenuse kiire taastumise ja minimaalse andmekao vastavalt taaste sihtkestusele ja taaste sihtseisule.

7.10. Liikmesriigid, Eurojust ja Euroopa Prokuratuur rakendavad eespool kirjeldatud käideldavuse eesmärkide saavutamiseks asjakohaseid meetmeid ja kehtestavad menetlused intsidentidele tõhusaks reageerimiseks.

8. **Pädevate asutuste/kohtute andmebaas**

8.1. Võttes arvesse määruse (EL) 2023/1543 artiklit 19, on detsentraliseeritud IT-süsteemi toimimiseks oluline luua usaldusväärne teenuseosutajate ja pädevate asutuste andmebaas.

8.2. Usaldusväärne pädevate asutuste andmebaas sisaldab struktureeritud kujul järgmist teavet:

a) määruse (EL) 2023/1543 artikli 19 kohaldamiseks teave pädevate asutuste kohta, kellest on teavitatud vastavalt kõnealuse määruse artikli 31 lõike 1 punktidele a–c, sealhulgas:

1) liikmesriike esindavad Eurojusti liikmed, sh teave selle kohta, kus nad võivad kooskõlas riigisisese õigusega teha Euroopa andmeesitamismäärusi ja Euroopa andmesäilitamismäärusi vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1727 ([7]) artikli 8 lõigetele 3 ja 4;

2) Euroopa delegaatprokurörid ja Euroopa prokurörid, kellest liikmesriigid on nõukogu määruse (EL) 2017/1939 ([8]) artikli 105 lõike 3 kohaselt teatanud kui pädevatest taotlevatest asutustest või ametiisikutest määruse (EL) 2023/1543 tähenduses;

b) asjakohasel juhul teave, mis on vajalik asutuste pädevuse geograafilise ulatuse kindlaksmääramiseks, või muud asjakohased kriteeriumid, mis on vajalikud asutuste pädevuse kindlaksmääramiseks;

c) teave, mis on vajalik detsentraliseeritud IT-süsteemi raames toimuva andmevahetuse nõuetekohaseks toimimiseks ja sõnumite tehniliseks marsruutimiseks.

8.2.1. Punkti 8.2 alapunktis c osutatud teave hõlmab järgmist:

a) teave liikmesriigi kohta, kus asub teenuseosutaja määratud majandusüksus või kus elab teenuseosutaja esindaja:

1) liikmesriik;

2) keskasutus;

([7]) Euroopa Parlamendi ja nõukogu 14. novembri 2018. aasta määrus (EL) 2018/1727 Euroopa Liidu Kriminaalõigusalase Koostöö Ameti (Eurojust) kohta ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsus 2002/187/JSK (ELT L 295, 21.11.2018, lk 138).

([8]) Nõukogu 12. oktoobri 2017. aasta määrus (EL) 2017/1939, millega rakendatakse tõhustatud koostööd Euroopa Prokuratuuri asutamisel (ELT L 283, 31.10.2017, lk 1).

b) teave teenuseosutaja kohta:

1) nimi;

2) aadress/asukoht;

3) registreerimisnumber;

4) õiguslik vorm;

5) telefoninumber;

6) e-post;

c) teave määratud majandusüksuse / esindaja kohta:

1) üksuse liik (määratud majandusüksus / esindaja);

2) nimi;

3) aadress/asukoht;

4) telefoninumber;

5) e-post;

6) üldine kontaktisik või -üksus;

7) teenuseosutaja / määratud majandusüksuse / esindaja aktsepteeritav(ad) ametlik(ud) keel(ed);

8) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2023/1544 ([9]) artikli 2 punktis 1 nimetatud teenused, mida pakutakse liidus;

9) nende ELi õiguslike vahendite liik, mille jaoks määratud majandusüksus / esindaja on määratud (olukordades, kus liikmesriigid ei kasuta kõiki asjaomaseid ELi õiguslikke vahendeid);

10) määramise / ametisse nimetamise territoriaalne ulatus;

d) teabe autentimine:

1) volitatud esindaja nimi;

2) ametinimetus;

3) aadress;

4) telefoninumber;

5) e-post;

6) kuupäev.

8.2.2. Kättesaadavuse korral võib punkti 8.2 alapunktis c osutatud teave sisaldada järgmist:

a) teave teenuseosutaja kohta:

1) kontaktisik teadete kohta päringute tegemiseks (kui see erineb allkirjastajast);

2) veebisait;

b) kättesaadavate andmete liigid:

1) iga asjaomase teenuse kohta:

— kättesaadavate andmete liigid;

— andmete kategooria;

— identifikaatorid;

— andmete kättesaadavuse periood;

([9]) Euroopa Parlamendi ja nõukogu 12. juuli 2023. aasta direktiiv (EL) 2023/1544, millega kehtestatakse määratud majandusüksuste määramise ja esindajate nimetamise ühtlustatud normid elektrooniliste tõendite kogumiseks kriminaalmenetluses (ELT L 191, 28.7.2023, lk 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) lisateave andmete kohta;

3) lisateave teenuse kohta (nt alltöövõtusuhted);

c) teave määratud majandusüksuse / esindaja kohta:

1) muud teenuseosutajad, kellega seoses see määratud majandusüksus või esindaja on määratud;

2) tehnilise abi kontaktandmed;

3) kontaktisik hädaolukordadeks;

d) tehniline teave:

1) tehnilise kontaktpunkti nimi;

2) tehnilise kontaktpunkti telefoninumber;

3) tehnilise kontaktpunkti e-posti aadress;

4) rakendusliidese URL, et teha andmete liikide kohta dünaamilisi infootsinguid;

5) ühenduse tüüp riikliku IT-süsteemiga:

— veebipõhine liides;

— rakendusliides;

— rakendusliidese tõuke-URL.

8.3. Seoses detsentraliseeritud IT-süsteemi tegevusvajadustega jagunevad ülesanded järgmiselt:

a) komisjon vastutab usaldusväärse andmebaasi arendamise, hooldamise, käitamise ja toetamise eest;

b) komisjon võimaldab usaldusväärsele andmebaasile juurdepääsu rakendusliidese kaudu, mis tehakse kättesaadavaks pädevatele asutustele, Eurojustile ja Euroopa Prokuratuurile, et nad saaksid osaleda detsentraliseeritud IT-süsteemis;

c) liikmesriigid tagavad, et punkti 8.2 alapunktides a ja b osutatud teave nende pädevate asutuste kohta on usaldusväärses andmebaasis täielik, täpne ja ajakohastatud;

d) usaldusväärne andmebaas võimaldab liikmesriikidel esitada ja ajakohastada teavet oma teenuseosutajate kohta ning detsentraliseeritud IT-süsteemis osalevatel asutustel sellele teabele programmi abil juurde pääseda ja seda välja otsida;

e) liikmesriigid ja teenuseosutajad tagavad, et punkti 8.2 alapunktis c osutatud teave on usaldusväärses andmebaasis täielik, täpne ja ajakohastatud.